Final Paper

Brandon Zakaras

Employer: Yogesh Sur

CYSE 368

Spring 2024

1

Table of Contents:

<div align="right">Brandon Scott Zakaras</div>

Final Paper:

Bottom Line Up Front:

I work as a COVA CCI Student Worker for my internship, which involves many different types of tasks for me to gain as much experience and knowledge as possible. This the final paper for my internship, where I explain the overall impact it has had on me, and what I have gained from it.

Introduction:

My major is Cybersecurity, and I am currently on track for a Bachelor's Degree at Old Dominion University. I have had an internship with the CCI ODU department since Fall 2023 semester, and this time has allowed me to continue to grow as a cybersecurity professional in multiple ways. My internship is directly with ODU, and I work in the Monarch Hall building, assisting with different cyber issues as they arise in the building. I am also given assignments by my two supervisors, Terry Stilwell and Yogesh Sur. I chose to do my internship with ODU for a few different reasons. First, I knew that they would understand my academic schedule, and allow me to focus on my schoolwork enough to maintain my grades. Second, a friend named Jose, who I respect, recommended me for this internship and I worked with him in the fall semester while I learned the ropes of what I would be doing. My internship didn't truly begin until this current semester though. In the Fall, even though I would work on the assignments given to me by Terry and Yogesh, if there were any problems in the building computer-related, then Jose would deal with it, and I would usually not be able to come along because of time constraints. This semester

all of that changed though, because Jose graduated and I took over the role that he had filled. Thus, as far as I am concerned, my internship truly began this semester, even though I have been working in the department for two semesters now.

When I first began my internship, I did not really know what to expect. I had never had a cybersecurity focused job before, so I based my expectations off of my college and high school classes. Therefore, I expected three things from my internship before I started. The first thing that I expected out of my internship was hands-on training in securing networks and actively trying to prevent red-team attacks. While this is not exactly what I got out of my internship, I did have the opportunity to learn how to theoretically build a network and the protocols and techniques needed to operate a low-level network. I believe that if I continue with this job until the end of my college career, then I could begin learning the real-time red-team examples that occur against Old Dominion's services. The second thing that I expected out of my internship was to learn more about how to hack, or infiltrate systems. I did not learn much about this topic in any official capacity, but one particular moment that I remember was an example of learning red-team hacking.

During one of my assignments that I was given, Linux 1, I had to restart multiple times, and also had many roadblocks that I needed help getting past. One of these was changing my password, because by this point I had made 10 different virtual machines for different assignments, and could no longer remember the password for my VM that I was using for that particular assignment. I was then taught how to change my password without needing the original, which could definitely be used in a red-team attack, especially if I was able to reach the device in person. The last of the three things that I was hoping to get out of this internship within the context of learning outcomes and objectives was a mentor that I could learn from directly,

and have a one-on-one relationship with so I could learn from someone with work experience outside of a classroom. In this department, I got more than I could have asked for. Because I have both Yogesh and Terry as bosses, I have two mentors. Each week I am able to go over with them what I have done, what I have not been able to do yet, and what has been giving me issues through Zoom meetings. Whatever has given me issues, they will guide me through and make sure that I understand what I am doing. Also, even though it is not on a perfect bi-weekly schedule, they will also come onto campus in person for our meetings so they can help me in person as well. So in this learning outcome that I was hoping to achieve, I could not have asked for a better result.

As previously stated, I didn't technically begin my internship this semester, but rather last semester, though there was a massive change in my duties and atmosphere when I came back. When I first started my internship, my role was slightly different. I inherently knew a good amount about where I was going to work, since I go to school at Old Dominion University. The part that I did not understand about my internship was the CCI branch that I would be working under. CCI stands for Commonwealth Cyber Initiative, and its main objective is to promote the advancement of cybersecurity in Virginia, and students wanting to learn more.

COVA CCI:

CCI is actually a relatively new initiative that was only established in July 2018, and the COVA part of COVA CCI stands for Coastal Virginia. The specific COVA branch of CCI focuses on research on Cyber Physical Systems Security, or CPSS for short, 5G, and Artificial Intelligence. It focuses this research on the Maritime, Defense, and Transportation business sectors. So even though I work with ODU, and COVA CCI, in truth I am actually a bit of both.

ODU Servers:

One of the aspects I did not know about though, was where all of the servers were stored that allow ODU to run all of the services it does. For context, cybersecurity students at Old Dominion University have to learn how to hack, so then they can know how their enemies will think, and where to defend the most. In order to safely learn how to hack, virtual machines, or VMs, must be used. To grossly simplify the idea of VMs for the sake of this essay, imagine a VM as an imaginary computer within a computer. A person can run a program on their computer that will create a smaller, more limited computer inside of it logically; and anything done within this VM will not affect the host machine. This is extremely important for cybersecurity majors and cybersecurity professionals, because it allows for viruses to be tested and infiltrating techniques to be practiced without the same types of dangers that are present on a physical machine. The only downside to this technique is that each person that wants to have a VM must have a powerful enough machine to run a VM. For example, a machine with 16 GB of RAM cannot make a virtual machine with 32 GB. It still takes up resources from a computer, it just doesn't affect the computer if the VM is infected or goes down. Now, the importance of this topic is all ODU students need to be able to use VMs in order to complete their core classes, in order to do the practicing that is required in order to be proficient in their field. All of this is important because I work right beside the servers that are used by those cybersecurity students, and am in charge of maintaining them if anything occurs that disrupts the natural flow of how they normally operate.

Last semester, I also worked with a Graduate student on his Master's project, which was also related to this topic. Currently, cybersecurity students use CCI environments that are dedicated to specific classes for their assignments, but the project by this student would have

made it possible for every cyberstudent to have access to their own personal VM hosted by ODU, to be able to practice on and use for their assignments, whatever they wished for. This was one of the primary focuses of my internship last semester, but sadly the student I was helping graduated at the end of the semester and his project has gone into a form of hiatus ever since. I did not get the opportunity to do much with assisting Old Dominion University employees last semester because of my shadowing Jose, so most of my job revolved around helping the Grad student, with me only assisting employees occasionally. Alongside this was my focusing on projects that I was given by Terry and Yogesh to further teach me the logic behind Linux, Networking, and DNS servers.

Management:

Terry and Yogesh are the bosses that I talk to the most, but the person I answer to above them is John Pratt. I rarely talk to John though, and most of my communication is with Terry and Yogesh through Teams and weekly Zoom meetings. They were the two people that did my initial interview when I was applying for the internship, so I have known them from the very beginning. While I have known them from the beginning, it took awhile for us to reach a point in my internship when we saw each other consistently in person. Part of the reason for this is that Terry and Yogesh currently work online only except for once a week when they come in, but last semester they worked in person in the ECS building, or the Engineering and Computational Sciences building, which is where another server room is that is used by all of Old Dominion University. They each had their own cubicle that they worked at, but I could not get my own spot in the building, so I chose to stay in Monarch Hall. Therefore, most of the communication was on Teams if I had any immediate questions that did not require in depth assistance, and Zoom was kept for every week on Thursdays. Through Teams, I would report my progress on

assignments and tickets that I had completed through the ODU Prod Service Now portal, which

is the portal that is used by Old Dominion University staff to report issues and request assistance.

I would also use Teams to ask Terry and Yogesh for assistance on my assignments, and on the

tickets I was working on if I ran into any issues. Then on Thursdays with the Zoom meetings, I

would walk through all that I had completed in the previous week, and they would both ensure

that not only had I completed what I was supposed to, but that I understood what I was doing in

order to reach my goal. Now even though I am considered a COVA CCI worker, I am also an

ODU IT worker, as I work on the tickets for the ODU Prod ServiceNow Portal, so I have

coworkers as well in other buildings. When I ran into problems with the tickets I did in my first

50 and 100 hours in this internship of this semester, my co-workers from the other buildings

helped me learn what I needed to do in order to complete the ticket. I technically have the

support of the IT help desk on the first floor, and two IT workers, Ryan O'Byrne and Aaron

Sadhoff, both assisted me in learning how to wipe a device and then connect it to ODU's InTune

service. There is also one more employee that assisted me on those tickets, and he works in the

Health Sciences Building, and his name is Matt Soricelli. I gave these names and where they

work to show that, even though I am the only student who works in Monarch Hall and I have two

bosses that I answer to, I do have coworkers that I reach out to and communicate with.

Work Duties:

As I have explained in minor details in the past paragraphs, my job has a few varying

duties, and I have some that are more local and do not require official definitions. My official

duties involve working on assignments given to me by Terry and Yogesh, including assignments

focused on Linux, Windows, and Networking.(Please look at Appendixes A, B, and C) They also

include working on any tickets assigned to my name under the ODU Prod Service Now Portal.

Sometimes these tickets are officially submitted, and sometimes I complete them before they have the chance to be officially submitted, and so they do not show in the system. These assignments help me understand how to better do my job in the future, and what goes into the systems that I will work with once I graduate. There is no guarantee that the place I will work will only use Windows machines or only Linux devices, and I must also understand how to build a network in case that is the role I am given in the company I work for. Understanding DNS and SSL, two other assignments that I have previously done, also help me understand how websites and the Domain Naming Service work and why they are so important to keep secure.

Previous Skills:

My understanding of networks, the Windows operating system, and Linux assisted me in my completion of my assignments, and some of this knowledge I had before I started at my internship. I had a basic understanding of how Windows and Linux worked, including command prompt and the basic commands to use in order to ping and understand IP addresses. In terms of networking, I understood a good amount of how a network is handled and created, because in my high school Cybersecurity class, half of my class had to build a network and secure it against the other half of the class. This helped me understand how computers are connected, and what they need to communicate. It also assisted in my understanding the importance of DHCP, DNS, and AD. The tasks given to me helped evolve my basic understanding into much more. In high school, I was given limited access to the Windows Server GUI, and parts of it were already set up for me. In the assignment I had to complete for this internship however, I had to understand how to make full groups, organizational units, group policy objects, and how to write scripts in powershell. I had not done most of this before my internship so this was a new focus for me, and I learned quite a bit from that assignment. For my Networking assignment I had never done an

motd before, or configured a Cisco device to request a password at the console screen. I

understood the basics of connecting devices to a network, but not how to make the network more

functional and have it be practical. The Linux assignment was probably the most insightful for

me, even despite the fact that most of the work given to me in the classes I have taken at ODU

have revolved around using Linux. Learning how to download source code and compile it from

scratch was one of the hardest tasks I was given this semester. It took me almost three to four

weeks to get past that part in my assignment, partially because I didn't have a clue of where to

look. In this assignment, Terry and Yogesh had to assist me in finding a website that helped me

understand where to find all the source code that I needed for my Linux assignment, and the

name of the website is called *Linux From Scratch*. Once I was able to begin finding the source

code, I thought I had finally figured out everything there was to know about downloading and

compiling, but I wasn't even close. When I began installing and attempting to compile most of

the programs, I realized, just as the assignment had stated, that most programs have another

program that they also require in order to run correctly. I then learned that one of the core

programs to install first is called GCC, and that this is a core program for many of the other basic

programs that most Linux users take for granted. Because of the grueling task of determining

how to compile the amount of programs I had to, and realizing just how many dependencies they

all had, and how it could all go wrong with one mistake, I learned the significance behind

package managers. Package managers take all of the strain off of the user and allow them to just

request a specific program, such as "ipconfig," and the package manager downloads all of the

required dependencies and then downloads and compiles the requested program. Another new

topic that I learned while doing that assignment was the importance of LVM for Virtual

Machines. LVM stands for Logical Volume Manager, and in simple terms, it allows for multiple

physical volumes of space to be combined into one logical volume. As an example, let's take Hard Drive A and Hard Drive B and plug them into the same machine. The LVM allows for the machine to combine both of these hard drives together, and consider them as only one hard drive, called Hard Drive C for the sake of this example. I was taught how to use the LVM in order to enlarge the amount of space I had on my VM while working on this assignment, ironically while I was working on the downloading and compiling section.

ODU Curriculum:

The ODU curriculum did well to prepare me for my internship. Quite a few of my networking classes taught me about DNS and how ethernet works. It taught me about the OSI layers of a network, and what goes into each. I also had an Ethical Hacking and Penetration class, along with an Intro to Linux class. Both of these classes helped me in understanding how Linux works, and how to operate within the operating system. Even simple things such as how to end a running program or navigating directories and opening files. Ironically, sometimes it would feel like my classes and internship went hand in hand without ever being in contact with each other. An easy memory was from only a month ago, when I was going over DNS with Terry and Yogesh, and I had to discuss with them the difference between a Recursive DNS server, and a Root DNS server. Only a few days earlier, I had gone over that very topic in a slideshow for the topic I was involved in, in my Cybersecurity Fundamentals class.

Objectives:

The objectives that I first stated in my paper, which were hoping for hands-on training in securing networks and actively trying to prevent red-team attacks, to learn more about how to hack, or infiltrate systems, a mentor that I could learn from directly, and have a one-on-one

relationship with so I could learn from someone with work experience outside of a classroom, were all fulfilled in one way or another. While I may not have gotten the conventional hands-on training I first expected when I joined this internship, I did wind up getting it in a different way.

The weekly meetings and both of my supervisors constant willingness to help me in any shortcomings I had when completing tasks was another form of the hands-on training I was hoping for, and by practicing my networking skills on the assignments I have been given, I have been learning how to secure a networking environment and protect it from outside sources. In terms of learning how to hack and infiltrate systems, I accidentally had to learn how to hack from Terry in order to break into my own Virtual Machine. I forgot the password to my Linux machine, and could not get back in to continue working on my assignment. Terry helped me load the ISO for Linux again, and inside of the Linux ISO launch screen, I was able to access the command prompt and change my password through there, without any account permissions. Therefore, in a sense, I was able to learn a form of red team hacking and infiltration. In terms of having a mentor to teach me directly and have a one-on-one relationship with, I got that in bucketloads. Not only did I wind up with one mentor, but two. Terry and Yogesh have each treated me with the utmost respect, and are always willing to help me out when I need it. They always invite me to meetings and seminars that are outside of my internship, in case I would like to learn more about the field I am hoping to go into. They are also happy to go out for lunch and discuss what I have been working on, making it an enjoyable experience. I could not ask for a better fulfillment of that objective.

Reflection:

This internship has definitely had its ups and downs for sure, but the consistent possibility for new experiences and the knowledge of a supporting hand if I do not understand

something makes this internship exciting and motivating. My supervisors always ask me if I am interested in any new topics, and if I tell them of any topics I am interested in, we discuss potential new assignments related to that topic, so I can continue to learn about it. The most discouraging aspect of this internship is when I have a difficult time completing one of my assignments or tasks, and don't understand why. I expect myself to understand what I am doing, and if I don't, then I begin to get disheartened. This is easily the hardest emotional part for me, but my supervisors are always supportive, and make this part of the internship pretty easy to bear. The most intellectually challenging part of my internship is learning how the ODU Prod Service Now portal works. I was never given a tutorial or guide on how to operate within the portal, so it has been a slow growth of understanding on how it works, and how to operate, and each time I use it I get a little bit better at using and understanding it.

Recommendations:

If I were to give my recommendations to any future interns looking to start this internship, my first would be to ensure that they are willing to dedicate themselves to Cybersecurity and understand more about it. It takes discipline to do this internship, because the supervisors trust you to do your job, and don't hold your hand the whole time you are working. I would also recommend understanding the basics of networking, command prompt, and Linux. As long as they understand these things, and are willing to have the discipline and resolve to work hard and not be distracted easily, then I think they would make great future interns and fair greatly in this environment.

Conclusion:

This internship has been beneficial to me for the entire time I have been a part of it. Without this experience, I do not believe that my time at ODU would have been nearly as effective toward my future career. My time with the COVA CCI department has helped refine the knowledge given by my classes, and gone more in depth on other items never taught in the classroom. I hope to continue my internship another semester, or continue at least working in the same field. By continuing to work in the same area, I will hopefully be able to further the growth of my knowledge and learn outside of the classroom on topics that are not discussed by the ODU curriculum. After I graduate, I hope to continue to use what I have learned here by ideally either going into penetration testing, or being a network supervisor. This internship has been one of, if not the, best part of my experience at Old Dominion University.

14

References

Costanzo, J. (2023, March 22). *Commonwealth Cyber Initiative*. Covacci.org.

https://covacci.org/

Welcome to linux from scratch!. Welcome to Linux From Scratch! (n.d.).

https://www.linuxfromscratch.org/

Appendix A

Linux Assignment

The following three extended references are references to Linux, Windows, and Networking

assignments that I have completed this semester, respectively.

This is my Linux assignment:

" – Setup /linux1 as an NFS share point on your first server

– Build another Ubuntu machine, it can be a desktop edition or server.

– Ensure that only your second server can mount the NFS share.

– Install a syslog server of your choice on the first server

– Setup syslog to send log data from your second machine to your first server

– Configure logs to "rotate" every hour.

– Write a bash script that appends the system's Current Time + Date, Load Average, Current Memory Usage, and the system's current uptime into a file. This script should run once every three minutes and should append data to the file. Use the system's scheduler. Mount the NFS share you created into your client's /linux1 folder. Setup syslog to log messages to your server.

– Attach a second disk to one of your servers through VCenter and use it to expand your / partition's space

(Don't share these answers with other consultants!)

– Find all files with SGID or SUID bits set

find / -perm -2000 -o -perm -4000 -exec ls -l {} +

– Why do they have them?

It seems to be that all of the files that are used by the user to change core system functions are given an SGID or SUID, most likely so then the system can pass on the permissions of the single person or group that owns the program, to the rest of the users of the system.

– Find out if your system uses systemd, init, or upstart. What are these? Things to know (These are hints as well):

Systemd (What is it)???

– What is LVM? Why would one use it? Relationship between LV, VG, PV?

LVM stands for Logical Volume Management. This is used to either separate or combine physical volumes (physical pieces of hardware that can hold data) into a "logical" volume, or how the computer views the volume in its mind, the system, where we as cyber personnel work. LV stands for Logical Volume, which is the container that holds a certain amount of data size according to what the computer can see. VG stands for Volume Groups, which are what is used to combine multiple volumes from different physical "drives" into one drive as far as the computer is concerned. PV stands for Physical Volume, and that is what each physical drive is.

– What is the difference between LVM and RAID?

LVM stands for Logical Volume Manager, whereas RAID stands for Redundant Array of Independent Disks. LVM combines multiple physical drives for easier use, whereas RAID combines everything into one unit, and is in charge of separating data into the different volumes, and keeping everything together. RAID also makes copies of data and stores it in different parts of the single unit, for data redundancy.

– What is Linux's equivalent to Windows Task Scheduler?

Cron, which was used in this assignment to schedule the rotating of files. In order to edit it, you used the command 'crontab -e'

– Where does the 'top' program get its information? -> Where else can you get the information presented in 'top'?

Top gets its information from "/proc" which is the directory for 'procfs', which stands for process file system. Other programs that act similarly to top are, 'ps', 'htop', 'nmon'. "Ps" is a screenshot method instead, showing a "screenshot" of the current statistics. "Htop" is a more user-friendly experience. "Nmon" does the same thing as "top", but is more geared towards system administrators and performance analysts.

– Where are logs stored?

All logs are held under the '/var/log' directory. After getting to this directory, then you can find the specific log that you are searching for.

– What's the difference between /bin and /sbin?

"/bin" and "/sbin" are both binary source code programs, but "/bin" holds programs that can be used by any user on the computer, and "/sbin" holds programs to be used by administrators or certain commands that can only be used when using 'sudo'.

– What's the use of SGID and SUID bits?

To grant users the ability to run a program with a higher privilege than their profile would ordinarily allow for. SGID is for a specified group of users, and SUID is for specified users.

– What is inside /dev? What are some of the different file types found in /dev?

The '/dev/' directory holds special files for the different devices that programs interface with, and the files are the method for which the programs can 'see' the device. No user can see view or write on these files, they are strictly for programs to interact with. "

Appendix B

Networking Assignment

This is my Networking assignment:

"Description:

Welcome to the world of networking. In this project you will learn about the basics of how all networks work, and you will create a small network to demonstrate what you have learned. Afterwards you will be quizzed on what this project covers, so please make sure you have a good understanding of the topics before taking the quiz.

For each networking project you will use Cisco's Packet Tracer, a tool used for simulating networks. Before you start the packet tracer part of the project, take a few minutes to play around with it to see what it can do, and get familiar with it. Everything you do to configure the devices will be through the device CLI, not the config tab. If you decide to use the config tab, it will be obvious you did and you might be asked to redo the project.

Scenario:

You have just been hired as the sole network engineer for a small business called the Ithavoll Group. Congrats! Your boss has decided that he wants a lab environment to test their program they are developing. He wants 5 computers in a room to all be able to talk to each other locally, and since they are just testing computers, they don't need Internet access. Your security team wants you to make sure to secure the devices properly, even though they are not connected to the Internet. Since this is your first time working with this stuff, you would want to get familiar with the different kinds of physical components a network would use as well.

Task:

Create a small network of 5 computers that can talk to each other locally. Use whatever IP addressing scheme you want, but make sure you are not wasting unnecessary IP address space in your subnet. Configure each Cisco device you use to prompt you for a password at the console screen, have an enable password, a basic motd, and encrypt every password in the running configuration. Do not use the initial auto-configuration. Do some research on copper cabling standards and connectors.

Appendix C

Windows Assignment

And this is my Windows Assignment:

"Your goal for this project is to become familiar with administering a Windows Server

2016 domain controller. You will deploy a domain controller, and use it to manage

Active Directory and Group Policy. You will also learn some basic scripting and remote

management.

Initial Tasks:

1. Deploy a Windows Server 2016 machine
2. Activate it using the standard volume license key.
3. Run Windows Update and apply all available patches.
4. Make the machine a domain controller with DNS capabilities, and create a domain for yourself: (<yourdomain>.cci.odu.edu) for which this machine is the first domain controller.
   Active Directory is a Directory Service for Windows domain networks. The following tasks apply to the Active Directory portion of the project.
   a. Create the following Organizational Units
      i. Computer Labs
         1. Problem Solving Lab
         2. Systems Staff Lab
      ii. Faculty
      iii. New Machines
      iv. Students
      v. Systems Staff
   b. Create corresponding Security Groups inside each of the OUs you just made except for the "Computer Labs" OU's
   c. Create seven total user accounts. Two will be faculty members, two will be Systems staff, and three will be students. Place them in the correct OUs and security groups.
      i. Members of the Systems Staff group should be able to reset the passwords of users in the "Students" OU. (Do not use the Builtin Account Operators group).
   d. Ensure that any new machines that are joined to your domain are automatically placed in the "New Machines" OU instead of the Computers container.
   e. Create a Windows 10 client and join it to your domain. After this, create and join two more Windows 10 clients to your domain. You may clone the first

machine you created if you wish. One machine will be a Systems Staff machine, and the other two will be in the Problem Solving Lab. Make sure that all computer accounts are members of their corresponding security groups and OUs. All machines should have hostnames that clearly identify their role in your organization.

    f. Ensure that all your Users, Groups, Computers, and OUs are protected from accidental deletion.

5. Group Policy is a robust tool in modern Windows operating systems that is used to configure the working environment for user and computer accounts. Configure the following for Group Policy:

    a. Make the following changes to the Default Domain Group Policy Object:

        i. Modify password policy

        ii. Make the following changes to a Group Policy Object with a name of your choosing that will affect your entire organization

            1. Groups allowed to use Remote Desktop

                a. Use the Domain Users group

            2. Which events should be audited

            3. Login Screen Message

            4. Configure it to use a NTP Server

        iii. Make the following changes to a Group Policy Object with a name of your choosing that will affect all Computer Labs:

            1. Who can shut down the machines in the labs

                a. Should be Systems Staff and Administrators only

            2. Users/Groups allowed to logon locally

                a. Administrators, Systems staff, Faculty, Students

        iv. Make the following Changes to a Group Policy Object with a name of your choosing that will affect the Systems Staff Lab:

            1. Users/Groups allowed to logon locally

                a. Should be Systems Staff and Administrators only

            2. Modify the membership of the Remote Desktop Users group

                a. Should be Systems Staff and Administrators only.

            3. Make the following changes to a Group Policy Object with a name of your choosing that will affect all students:

                a. Software installation that publishes a program of your choosing

                Scripting is a useful way to automate routine tasks. Create and configure the following script:

                    i. An account creation script written in Powershell that will create a new user in the Domain Users group and set its password. The input will be first name, last name, username, and password. This script should read from a file formatted as such: firstname,lastname,username,password
It should also be capable of looping through any number of users in the file.

6. Microsoft provides tools that make the remote management of computers in your organization incredibly simple. Complete the following for the Remote Management portion of the project:
    a. Install the Remote Server Administration Tools on the Systems Staff machine and ensure that you can use it to manage the roles and services on your domain controller remotely."